BUNDESREPUBLIK DEUTSCHLAND

Bescheinigung

Die International Business Machines Corporation in Armonk, N.Y./V.St.A. hat eine Patentanmeldung unter der Bezeichnung

"Hardwarenahe Konfiguration und Verriegelung von Geräten"

am 24. September 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole G 07 C und G 06 F der Internationalen Patentklassifikation erhalten.

München, den 9. Mai 2000

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Weihmayr

Aktenzeichen: 199 45 861.8

B E S C H R E I B U N G

HARDWARENAHE KONFIGURATION UND VERRIEGELUNG VON GERÄTEN

1. HINTERGRUND DER ERFINDUNG

1.1 GEBIET DER ERFINDUNG

Die vorliegende Erfindung betrifft Verfahren und Vorrichtung zum Festlegen grundlegender Verfügungsmöglichkeiten über den Betrieb von elektronisch angesteuerten Geräten, insbesondere betrifft sie Verfahren und Vorrichtung zum Konfigurieren und Verriegeln von Geräten mithilfe einer personenbeziehbaren Authentisierungseinrichtung, insbesondere mithilfe von SmartCards.

1.2. NACHTEILE DES STANDES DER TECHNIK

Der Begriff 'Gerät' wird im Zusammenhang mit den hier vorgestellten, erfinderischen Konzepten sehr breit und allgemein verstanden. Es handelt sich um eine Vielzahl von Geräten, vom kleinen Handy oder anderen kleinen, computergesteuerten Gebrauchsgeräten mit einer gewissen, vergleichsweise geringen Rechenleistung über eigentliche Computer bis zu größeren 'Geräten' wie Kraftfahrzeuge bis hin zu Steuerterminals für industrielle Prozesse, die einer Authentisierungsüberprüfung vor einer Betriebsaufnahme bedürfen könnten. Als Voraussetzung muß allerdings jedes dieser Geräte über eine elektronische Steuerung verfügen, die den Betrieb des Geräts ermöglicht, was heute allerdings fast überall anzutreffen ist.

Die individuelle Konfiguration von Geräten ist eine wichtige Aufgabe bei kundenorientierten Fertigungsprozessen. Dabei werden im Stand der Technik drei grundsätzliche Konfigurationsmechanismen angewandt.

Zum einen können die Geräte bereits werksseitig für individuelle Kunden eingestellt werden. Die benötigte Software wird bei der Herstellung in das Gerät geladen. Dies setzt allerdings präzise geplante Produktionsprozesse mit aufwendigen Produktionsplanungssystemen voraus, die oft nicht gegeben sind und erhöht die Lieferzeiten.

Zweitens kann die Konfiguration der Geräte dem Kunden delegiert werden. Er kann beispielsweise mit einer Installationsdiskette sein Gerät individuell einstellen. Der Mehraufwand für den Kunden kann dabei allerdings zu erheblichen Wettbewerbsnachteilen führen, da er in die Programmierlogik der Geräte nicht eingearbeitet ist. Außerdem wirft die Vorgehensweise Sicherheitsfragen auf, insbesondere, wenn es sich bei den zu konfigurierenden Funktionen um aus betrieblicher Sicht kritische Funktionen handelt oder wenn dabei vom Hersteller des Gerätes interne Informationen über das Produkt bekanntgegeben werden müssen. Die Weitergabe dieser Konfigurationsinformationen kann nicht kontrolliert werden.

Zum Dritten nutzen viele Anbieter Online-Verbindungen, wie beispielsweise das Internet oder das Telefon für die individuelle Konfiguration von Geräten oder Anlagen, bestehend aus vielen solchen Geräten. Dies ist beispielsweise für Telefonanlagen relevant: Moderne Telefone sind heute meist mit der maximal möglichen Funktionalität ausgestattet, haben aber nur die Leistungsmerkmale aktiviert, die vom Kunden bestellt und bezahlt wurden. Das Gerät kann damit in großen Stückzahlen identisch produziert werden und muss erst vor Ort beim Kunden konfiguriert und personalisiert werden.

Ein nachträgliches Erneuern der Software bei den Telefonanlagen über solche Online-Verbindungen ist derzeit sicherlich die flexibelste Möglichkeit, setzt aber voraus,

dass genaue Informationen über den Kunden und seine betriebliche Konfiguration vorliegen, was oft nicht gegeben ist.

Auch Aspekte wie Datenschutz der Konfigurationsdaten bei einem Weiterverkauf der Anlage, etc., müssen hierbei jedoch in Betracht gezogen werden. Diese Sicherheitsaspekte können nur beschränkt berücksichtigt werden, etwa durch ein Passwort beim Anmelden am Konfigurationsserver des Herstellers oder Serviceproviders und einem Abmelden am Ende der Online-Verbindung.

Die oben genannte, erste Möglichkeit ist für den Hersteller extrem aufwendig und kostenintensiv, insbesondere bei preiswerten Geräten der Unterhaltungselektronik.

Bei den zwei zuletzt genannten Varianten ist nur schwer sicherzustellen, dass Nutzer des Geräts nicht unberechtigterweise bestimmte Konfigurationen nutzen oder weiterleiten, für die sie nicht berechtigt sind.

Technisch oft eng verzahnt mit der Möglichkeit, Geräte zu konfigurieren, ist die Möglichkeit, diese Geräte so zu 'konfigurieren', daß sie verriegelt und keiner normalen Benutzung mehr zugänglich sind.

Eine Möglichkeit im Stand der Technik, die Hardware solcher Geräte zu verriegeln und so die Geräte vor Missbrauch oder Diebstahl zu schützen, ist von Mobiltelefonen und PCs her bekannt.

Die dort angewandten Verfahren, bestehen aber lediglich aus der Eingabe eines Passworts. Daraus resultieren Risiken des Missbrauchs, wenn das Passwort bekannt wird. Außerdem kann beispielsweise ein 4-stelliger Code, welcher heute beim

Mobiltelefon verwendet wird, computergestützt schnell 'geknackt' werden.

Weiter ist der Bedienerkomfort gering, denn das Passwort kann leicht vergessen werden.

Komplexere Schließfunktionen, die nicht so leicht zu entschlüsseln sind, und die kryptographische Schlüssel und verschiedene Rollen wie Anwender, Servicetechniker oder Systemadministrator definieren, sind bei den existierenden Verfahren nicht möglich.

Sobald Geräte des Standes der Technik komplexere, auf Smartcards basierende Sicherheitsmerkmale aufweisen, sind diese Anwendungen im Stand der Technik als Software implementiert. So bietet beispielsweise bei PCs das Betriebssystem Windows 2000 einem mit dem PC assoziierten Smartcardbesitzer die Möglichkeit, individuelle Zugriffsrechte für verschiedene Dateien zu definieren und individuelle Konfigurationen einzustellen. Dieses Verfahren setzt allerdings auf dem Betriebssystem auf und kann durch Löschen des Betriebssystems auf der Festplatte inaktiviert werden. Ein potentieller Dieb kann nach erneutem Installieren des Betriebssystems bzw. nach Austausch der Festplatte das System uneingeschränkt nutzen. Lediglich die Daten des Anwenders können mit dem bestehenden Verfahren weitgehend geschützt werden.

1.3. AUFGABEN DER ERFINDUNG

Daher besteht die Aufgabe der vorliegenden Erfindung darin, eine zuverlässigere Möglichkeit zu schaffen, derartige Geräte vor unbefugter Benutzung zu schützen, so dass sie für einen Dieb oder eine einen Gerätemißbrauch beabsichtigenden Person nicht mehr attraktiv sind.

Eine weitere Aufgabe besteht darin, derartige Geräte komfortabel und sicher konfigurierbar zu machen, d.h., sie einer individuellen Nutzung durch den Kunden zugänglich zu machen.

2. ZUSAMMENFASSUNG UND VORTEILE DER ERFINDUNG

Die genannten Aufgaben werden durch die in den unabhängigen Ansprüchen genannten Merkmale gelöst. Vorteilhafte Weiterbildungen des Erfindungsgegenstandes ergeben sich aus den jeweiligen Unteransprüchen.

Die hier vorgestellte, erfinderische Lösung basiert im wesentlichen auf drei Komponenten, um grundlegende Verfügungsmöglichkeiten, wie insbesondere die temporäre Stilllegung, die Inbetriebnahme oder Wieder-Inbetriebnahme sowie die Konfiguration von Geräten festzulegen, nämlich:
einer Erweiterung der Gerätehardware um Funktionen, die grundlegende Verfügungsmöglichkeiten über den Betrieb von Geräten, nämlich insbesondere die individuelle Konfiguration und die Stilllegung der Geräte erlauben,
einer hardwarenahen Schnittstelle zu einem Lesegerät, wie etwa einem Smartcard-Reader, der den Zugriff auf diese Funktionen durch die Smartcard erlaubt, und
der Authentifizierungseinrichtung selbst, wie etwa eine Smartcard , die in der Lage ist, über die definierte Schnittstelle auf die Konfigurations-/ und/ oder Stilllegungs- bzw. (Wieder-) Inbetriebnahmefunktionen der Hardware des Gerätes unmittelbar zuzugreifen.

Die Legitimation zur Konfiguration /Stilllegung und (Wieder)-Inbetriebnahme des Geräts erfolgt vorzugsweise über den Abgleich von Schlüsseln, die auf der SmartCard bzw. vorzugsweise in einem ROM des Geräts gespeichert sind. Alternativ dazu oder in Kombination damit könnte dies aber

auch über andere, z.B., biometrische Authentifizierungsverfahren geschehen. Beispielsweise könnte ein Finderabdruck auf der Smart Card abgespeichert werden, der dann beim Reaktivieren des Gerätes verglichen wird.

Die erstgenannte Hardware-Erweiterung ist gerätespezifisch. Bei PCs etwa kann beispielsweise der Prozessor um derartige Funktionen erweitert oder das BIOS ergänzt werden. Bei Geräten der Unterhaltungselektronik oder Telefonen, könnten die Funktionen im ROM, bzw. in der Firmware definiert werden. Im Gerät müssen kryptographische Schlüssel hinterlegt werden, die bei Konfiguration, Stilllegung bzw. Wiederinbetriebnahme von der Smartcard zur Authentifizierung der berechtigten Person genutzt werden.

Die Schnittstelle zwischen Gerät und Smartcard beinhaltet einen gewöhnlichen Smartcard-Leser, der um eine hardwarenahe Steuerung erweitert wird, da die zur Ansteuerung üblichen Softwaretreiber bei dieser hardwarenahen Lösung erfindungsgemäß wegfallen. Hier ist eine Realisierung als ROM, BIOS oder Firmware als individuelle, 'in Hardware gegossene' Software grundsätzlich denkbar. Alternativ könnte statt der SmartCard und dem SmartCard Leser auch jeder andere sogenannte Secure Token, mit entsprechender Verbindung zum Gerät verwendet werden, wie etwa beispielsweise der eToken von Aladdin oder ein JavaRing von Dallas Semiconductor.

Die dritte der oben genannten Komponenten - die Authentisierungseinrichtung - ist als Smartcard ausgebildet sicherlich die flexibelste der drei Komponenten. Sie kann gegebenenfalls in vorteilhafter Weise von einer Person zu einer anderen übertragen werden, sofern dies gewünscht ist, und ist offen für abgestufte Hierarchien von Zugriffsrechten auf das Gerät, etwa durch Herstellen einer MasterSmartCard, die zum Zwecke der Konfiguration einer Vielzahl von Geräten

an Servicepersonal des Abnehmers der Geräte ausgegeben werden kann. So kann beispielweise bei Nutzung einer Smart Card sehr flexibel und sehr individuell die Logik programmiert werden, nach der das betrachtete Geräte konfiguriert, stillgelegt oder wieder in Betrieb genommen werden soll oder darf. Auf der Karte lassen sich nämlich sehr vielfältige Informationen speichern, wie etwa komplette, kundenindividuelle Firmware-Updates, gerätespezifische Befehlssequenzen, die bestimmte Funktionen am Gerät ausführen, wie etwa den Prozessor zu inaktivieren, kryptographische Schlüssel als Gegenstück zu den Schlüsseln im Gerät, mit denen eine individuelle Authentifizierung durchgeführt werden kann, wie etwa public key/ private key-Verfahren, kryptographische Algorithmen und individuelle Entscheidungslogik, und ggf. entsprechende Schlüssel, die den Kunden authorisieren, um zusätzliche Konfigurationsdaten oder Softwarekomponenten von einem Server des Herstellers zu laden, sowie die benötigten Daten um die Verbindung aufzubauen (z.B. Telefonnummer oder IP-Adresse).

Bei Anwendung des erfindungsgemäßen Verfahrens kann ein Gerätehersteller unter der Maßgabe, daß eine einzige SmartCard beliebige Geräte konfigurieren können soll, daß jedoch zum Zwecke der Stilllegung und/ oder der (Wieder-) Inbetriebnahme nur eine MasterSmartCard oder eine personenbezogene SmartCard verwendet werden kann, folgendermaßen vorgehen:

Ein Gerät wird in großen Stückzahlen identisch produziert. Jedes Gerät enthält kryptographische Schlüssel, die im ROM eingebrannt sind und für die Abwicklung von Authentisierungsprotokollen geeignet sind. Diese identischen Geräte ('white devices') können nun gelagert werden. Bei der Bestellung eines Kunden werden nun diese 'white devices' aus dem Lager entnommen und für jedes Gerät wird entsprechend den Bestellvorgaben des Kunden eine Smartcard mit den

Konfigurationsdaten erstellt. Diese Smartcard wird separat vom Gerät zum Kunden gesandt und ist praktisch der zu den Schlüsseln im Gerät passende kundenindividuelle Gegenschlüssel. Jedes Gerät kann damit mit der passenden Smartcard und/oder einer Master-Smartcard des Herstellers in Betrieb genommen und stillgelegt werden, kann jedoch mit der MasterSmartCard des Herstellers konfiguriert werden. Dies kann durch kryptographische Algorithmen seitens der Smartcard, wie beispielsweise asymmetrischer Authentisierung mit public und private Key RSA Algorithmen und hardwarenahen Funktionen seitens des Gerätes sichergestellt werden.

Sind die notwendigen Konfigurationsdaten zu umfangreich um vollständig auf einer Smartcard gespeichert zu werden, wie es z.B. bei einem PC denkbar ist, kann der Kunde das Gerät an ein mit dem Hersteller verbundenes Netzwerk oder auch an eine Telefonleitung anschließen und sich mit Hilfe der Smartcard für den Zugriff auf einen Konfigurationsserver des Herstellers authorisieren. Dazu ist eine Basissoftware zum Netzwerkanschluss und zum Download von Software vorzusehen. Die von Kunden bestellten Leistungsmerkmale des Geräts werden nun über die Smartcard aktiviert, und das Gerät lädt bei Bedarf fehlende oder neuere Softwarekomponenten über den Netzwerkanschluß oder die Telefonleitung.

Der Benutzer kann nun in vorteilhafter Weise zum Zwecke der Verriegelung des Geräts jederzeit das Gerät stilllegen, indem er die Smartcard zur Inaktivierung der Hardware nutzt. Somit ist das Gerät ideal vor Diebstahl oder Mißbrauch durch Dritte geschützt, wenn der Benutzer nicht anwesend ist. Ein Vergessen des Paßworts ist nicht möglich, da keines verwendet wird.

Für eine sichere Verriegelung müssen auf jedem einzelnen Gerät zusätzlich im Sinne einer Seriennummer individuelle, eindeutige Schlüssel, wie beispielsweise symmetrische

Authentisierung mit DES Algorithmen fest gespeichert werden, beispielsweise im ROM. Eine bestimmte, normale SmartCard kann nur das eine, ihr zugeordnete Gerät aktivieren bzw. stilllegen.

Weiter ergibt sich für den Hersteller eines Gerätes der Vorteil, daß er durch kryptographische Schlüssel sicherstellen kann, daß der Kunde nur diejenige Konfiguration nutzen kann, für die er berechtigt ist. Ein Mißbrauch von Konfigurationsdaten durch deren Weitergabe ist praktisch ausgeschlossen, da die Daten aufgrund der Verflechtung mit dem Sicherheitsschlüssel nicht zu einer anderen Anlage passen.

Damit ergeben sich wesentlich erhöhte Sicherheitsmerkmale bei Gerätekonfiguration und Gerätestilllegung gegenüber herkömmlicher Authorisierung/ Authentifizierung durch einen PIN.

Desweiteren lassen sich auf der Smartcard individuelle Kundeneinstellungen speichern, die der Anwender sehr individuell und off-line zum Konfigurieren seines Gerätes nutzen kann.

Der Kunde kann sein Geräte inaktivieren, z.B. bei längerer Nutzungspause während eines Urlaubs, und durch diese "elektronische Wegfahrsperre" sein Gerät für Diebe unattraktiv machen. Das Gerät ist so lange unbrauchbar, bis die Sperre mit derselben Karte oder einer Back-up-Karte vom Hersteller wieder aufgehoben wird.

Wesentlich an dem erfindungsgemäßen Verfahren ist, daß es direkt auf Hardware, bzw. BIOS-Ebene aufsetzt, und somit keine dazwischenliegenden Softwareschichten evtl. Sicherheitslücken entstehen können. Da die komplexe Entscheidungslogik, betreffend die Fragen, welche

Konfiguration und welche Zugriffsrechte anzuwenden sind, auf der Smartcard gespeichert werden, ist es möglich, diese geräteseitigen Vorbereitungen mit verhältnismäßig geringem Aufwand zu realisieren.

Das Verfahren ist aufgrund seiner Hardwarenähe in vorteilhafter Weise unabhängig davon, welche Software, Treiber und Betriebssysteme letztendlich auf dem Gerät installiert sind.

Der Hersteller erreicht schließlich durch dieses Verfahren einen vorteilhaften Investitionsschutz, da er keine Konfigurationsinformationen preisgegeben muß und sicher sein kann, daß das Gerät nur in dem mit dem Kunden vereinbarten und auf der SmartCard dokumentierten Umfang genutzt werden kann.

Bei der Produktion der Geräte muß nicht mehr auf die spezielle Konfiguration, die der Kunde wünscht, geachtet werden. Alle Geräte können identisch produziert werden, womit sich der Produktionsprozess vereinfacht und verbilligt. Außerdem lassen sich dadurch Lieferzeiten verkürzen, da nun die Geräte auf Lager produziert werden können, und bei Auslieferung mit einer bestimmten Konfiguration nur noch die Smartcard personalisiert werden muß. Wird ein Gerät dann an einen Kunden ausgeliefert, so wird eine Smartcard mit den Konfigurationswünschen und den vom Kunden verlangten Leistungsmerkmalen erstellt und dem Gerät beigelegt.

Geräte mit Netzwerkanschluß können sich bei der ersten Aktivierung die neuste Software zur Vervollständigung der Betriebsprogramme laden.

Der Kunde erzielt durch das erfindungsgemäße Verfahren einen Diebstahlschutz: Denn es macht keinen Sinn, ein Gerät auf

dem Transport oder während des Betriebs zu stehlen, da dieses ohne die Smartcard wertlos ist.

Letztlich wird die Handhabung des Konfigurationsprozesses deutlich vereinfacht.

Anwendungen dieses Verfahrens sind im folgenden nur beispielsweise genannt:

Diebstahlschutz für Personal Computer: Mit Hilfe der Smartcard kann ein Rechner bei Abwesenheit hardwareseitig verriegelt werden. Er ist dann so lange unbrauchbar, bis mit derselben Karte oder einer Backup-Karte vom Hersteller die Sperre wieder aufgehoben wird. Optimalen Schutz bietet das Verfahren durch Implementierung des rechnerseitigen Teils des Verfahrens direkt im Prozessor.

Vorteile ergeben sich auch bei der Wartung des PCs: Wird beim PC ein konventionelles Hardware-Password gesetzt, muß dieses Kennwort Servicetechnikern bekannt gemacht werden. Wird kein Password verwendet, ist dagegen das System nicht ausreichend geschützt.

Wird das Hardware-Password wie erfindungsgemäß vorgeschlagen durch Smartcards ersetzt, ist es möglich, verschiedenen Arten von Personenkreisen jeweils einen spezifischen Zugang zu gewähren: Dem Besitzer vollen Umfang und dem Techniker des Herstellers beispielsweise Zugang, ohne Plattenzugriffe zu erlauben.

Das Verfahren ist damit wesentlich leistungsfähiger, anwendungsfreundlicher, flexibler und sicherer als die Anwendung des herkömmlichen Hardware-Passworts.

Weiteres bevorzugtes Anwendungsgebiet ist das Konfigurationsmanagement für Telefone.

Telefone und andere elektronische Geräte, die in großer Stückzahl für verschiedene Märkte gebaut werden, müssen für die einzelnen Käufergruppen oder Kunden konfiguriert werden, z.B. hinsichtlich der Einstellung von Landessprache, anzuwendendem Verschlüsselungsverfahren, spezifischen länderspezifischen Protokollen, Funktionsumfang, wie oben erwähnt.

Der hardwarenahe Einsatz der Smartcard eröffnet hier neue flexible Möglichkeiten der Konfiguration, ähnlich wie oben beschrieben, die sich insbesondere für Privatkunden mit geringer Anzahl von Geräten anbietet, da dann alle Konfigurationsdaten direkt auf der SmartCard gespeichert sein können.

Auch Leasing oder Miete von Geräten können erfindungsgemäß verbessert werden, wenn die Nutzungserlaubnis durch Smartcards geregelt werden kann und nur mit einer gültigen Smartcard die Nutzung des Gerätes erlaubt wird.

Geräte mit Netzwerkanschluß können nur mit der zum Netzzugriff nötigen Basissoftware ausgeliefert werden. Bei der Konfiguration lädt das Gerät dann die aktuellen Softwaremodule von einem zentralen Server.

Die erwähnten Geräte oder deren Konfigurationen können noch zusätzlich dadurch geschützt werden, daß auf der SmartCard ein oder mehrere persönliche Kennwörter für einen, bzw. mehrere, vorbestimmte Benutzter gespeichert sind.

Somit kann ein Mißbrauch des Geräts auch nach Verlust der SmartCard vorerst verhindert werden, da ein unberechtigter Finder der SmartCard das oder die Paßwörter nicht kennt.

3.ZEICHNUNGEN

Fig. 1 zeigt ein schematisches Blockdiagramm eines Gerätes in Form eines Notebooks, das nach dem Verfahren bzw. Vorrichtung der vorliegenden Erfindung gegen unbefugte Benutzung verriegelt werden kann,

Fig. 2 zeigt den Steuerfluß bei einer komfortablen und sicheren Konfiguration einer Gerätegruppe, nämlich einer Telefonanlage, die in einem Unternehmen installiert ist.

4. GENAUE BESCHREIBUNG DER AUSFÜHRUNGSBEISPIELE

In Fig. 1 ist als Teil der Hauptplatine 10 eines Notebooks 12, die als wesentliches, durch das erfinderische Konzept zu schützendes Aggregat des Notebooks in Relation zu Peripheriegeräten betrachtet wird, das BIOS ROM 14 abgebildet. Erfindungsgemäß ist im BIOS oder alternativ beispielsweise im Prozessor selbst ein längerer Schlüssel gespeichert, der zur Authentifizierung des rechtmäßigen Benutzers verwendet wird. Das Gegenstück zu dem Schlüssel ist auf einer SmartCard 16 gespeichert, die über einen zwischen BIOS und SmartCard geschalteten SmartCard Reader 18 ansprechbar ist. Die Smartcard wirkt mit einem im BIOS des Gerätes erfindungsgemäß vorgesehenen Benutzerauthentifizierungsprogramm über ein vereinbartes Protokoll, z.B., ISO 7816-4 konforme APDUs für SmartCards als gemeinsame Schnittstelle zusammen. Befehle und Daten können somit zwischen dem BIOS Programm und der SmartCard ausgetauscht werden und je nach Implementierungsweise Folgebefehle anstoßen, die weitere Aktionen ermöglichen, die über die reine Token- oder ggf. Benutzeridentifizierung und Freigabe des Betriebs des Geräts oder Stilllegung des Geräts hinausgehen. Dieses hardwarenahe Authentifizierungsprogramm stellt daher eine Hardware-Erweiterung 20 in Form einer Hardwaresteuerung dar, die den Betrieb oder bestimmte

Betriebsarten von Geräten steuert. Dabei sind vorzugsweise für die auf der Smart Card gespeicherte User-ID eine Auswahl an grundlegenden Verfügungsmöglichkeiten gespeichert, die nach erfolgter Authentitätsprüfung freigegeben werden.

Soll das Notebook 12 nun in Betrieb genommen werden, so startet beim Einschalten das im BIOS 14 gespeicherte Authentifizierungsprogramm und verlangt, daß eine passende SmartCard 16 in den Reader 18 eingeschoben wird. Es wird nun erfindungsgemäß eine Verbindung 19 zwischen SMART Card und der Hardware-Erweiterung 20 unter Einbeziehung des BIOS ROMs 14 aufgebaut.

Diese Verbindung ist physikalisch als fest verdrahtet und logisch als 'sicher' im Sinne einer Umgehung, Fälschung oder einer Außerkraftsetzung der Authentitätsprüfung anzusehen. In besonders bevorzugter Weise wird daher diese Verbindung als reine Hardware-Implementierung unter Vermeidung jeglicher, zwischenliegender Software, wie etwa einem Gerätetreiber für den SmartCard-Leser 18 aufgebaut.

Dann wird die Eingabe einer Benutzerkennung und eines zugehörigen Paßworts vom Programm verlangt. Der rechtmäßige Benutzer kennt diese Daten und gibt sie über die Tastatur des Notebooks ein. Bei unkorrekter Eingabe der beiden Ausdrücke wird der Vorgang wiederholt und nach einer vorgegebenen Anzahl von Malen abgebrochen, z.B. nach dreimaliger Eingabe.

Nach korrekter Eingabe prüft das Programm im BIOS, ob der Schlüssel im BIOS zu dem Schlüssel auf der SmartCard paßt. Die Schlüssel können nach gängigen, anerkannten Mechanismen gebildet und verglichen werden, z.B. nach dem public key / private key Verfahren. Passen die Schlüssel, so erlaubt das BIOS-Programm dem Benutzer diejenigen grundlegenden

Funktionen, die für ihn auf der Karte als 'erlaubt' gespeichert sind.

In diesem Falle gibt das BIOS Programm durch Abgabe eines entsprechenden Signals an den Prozessor, der im weitesten Sinne als die eingangs genannte, elektronische Gerätesteuerung angesehen werden kann, den Betrieb des Notebooks frei und bootet es.

Passen die Schlüssel nicht, wird der Rechner dem Resultat entsprechend nicht gestartet. Der Rechner kann dann nur durch Einführen der SmartCard mit dem richtigen Schlüssel darauf gestartet werden. Andernfalls ist er unbrauchbar, da er nur durch Austausch der gesamten Mutterplatine 10 von dem Sicherheitsmechanismus abgekoppelt werden könnte.

Dies stellt eine beachtlichen Fortschritt im Vergleich zum Stand der Technik dar, bei dem lediglich durch Neu-Installation des Betriebssystems oder Abklemmen und Wiedereinsetzen der Batterie des Rechners der Rechner unbefugt verwendet werden kann. Daher ist ein solchermaßen geschützter Rechner weniger diebstahlgefährdet als solche vom Stand der Technik.

Auch ein Palmtop Gerät 22 oder dergleichen könnte anstatt der SMART Card an entsprechende Anschlüsse im Notebook angeschlossen werden, um die gleichen Funktionen wie die der o.g. SMART Card und möglicherweise noch zusätzliche Funktionen je nach Einsatzzweck des Gerätes 12 zu erfüllen.

Im Zusammenhang mit **Fig. 2** wird nun ein besonders bevorzugtes Merkmal beschrieben, wie unter Einsatz der erfinderischen Konzepte auch von der SmartCard selbst verschiedene Aktionen initiiert werden können, die unter anderem zur komfortablen Konfiguration von Geräten ausgenutzt werden können.

Eine Telefonanlage für ein Unternehmen besteht aus 20 Telefonen, die hierarchisch in 3 Schichten eingruppiert sind und entsprechend unterschiedlichen Funktionsumfang besitzen. Die Telefonapparate selbst werden einheitlich produziert und erhalten ihre eigentlichen Leistungsmerkmale erst durch eine Konfigurationsprozedur, die verschiedene Logikbauteile in den Apparaten in Betrieb setzt oder gesperrt lässt, je nach den individuellen Anforderungen des Kunden. Der Hersteller der Telefonanlage liefert nun mit der Anlage eine SMARTCard, die als MasterSmartCard ausgebildet ist und diese Konfigurationsprozedur anstößt, wenn sie in ein entsprechendes Schnittstellengerät eingeschoben wird, Schritt 110, einem SmartCard-Reader, dessen Ausgang mit der Telefonanlage verbunden ist.

Dann wird, wie oben im Zusammenhang mit Fig. 1 beschrieben, die Eingabe einer Benutzerkennung des SuperUsers und eines zugehörigen Paßworts vom Programm verlangt. Dies ist ein optionaler Schritt, da der auf der Smartcard gespeicherte Personenidentifizierungsschlüssel an sich auch schon ausreicht, um die Identität der Karte als MasterSmartCard zu erkennen. Der rechtmäßige Benutzer kennt die SuperUser-ID und das zugehörige Passwort und gibt sie über die Tastatur eines Telefons der Telefonanlage ein, Schritt 120. Bei unkorrekter Eingabe der beiden Ausdrücke wird der Vorgang wiederholt und nach einer vorgebenen Anzahl von Malen abgebrochen, z.B. nach dreimaliger Eingabe, Schritt 130.

Nach korrekter Eingabe prüft ein Authentifizierungsprogramm in einem ROM auf dem Chip des Telefons, ob der Schlüssel im ROM zu dem Schlüssel auf der SmartCard paßt, Schritt 140. Die Schlüssel können wie oben nach gängigen, anerkannten Mechanismen gebildet und verglichen werden, z.B. nach dem public key / private key Verfahren. Passen die Schlüssel, so gibt das Programm im ROM des Telefons die notwendigen

Funktionen frei, die notwendig sind, um die Telefonanlage konfigurieren zu können.

Auf der SmartCard sind nun alle notwendigen Daten gespeichert, die zur Initialisierung, Konfiguration und Personalisierung der einzelnen Telefonapparate in der Anlage notwendig sind. Diese werden daher von einem auf der Karte gespeicherten und ausführbaren Programm in Speicherplätze der Telefonanlage geschrieben, die dort vorgesehen sind, Schritt 150. Weiter ist ein Programm auf der SmartCard vorhanden, das die Konfigurationsprozedur enthält. Somit kann die gesamte Anlage mit den jeweils richtigen Leistungsmerkmalen konfiguriert werden.

Falls die Schlüssel nicht zueinander passen, wird die Prozedur abgebrochen und eine Konfiguration kann nicht stattfinden, siehe die Verzweigung zu Schritt 130.

In besonders bevorzugter Weise und in Erweiterung des in Fig. 2 beschriebenen Ausführungsbeispiels ist das erfinderische Verfahren zur Konfiguration von Geräten mit SMART Cards auch geeignet, Konfigurationen durchzuführen, die erheblich mehr Konfigurationsdaten benötigen, als auf eine SMART Card passen würden. Erfindungsgemäß wird dann vorgeschlagen, von der SmartCard einen Befehl abzusetzen, der eine Datenverbindung, wie z.B. eine TCP/IP Verbindung zu einem Datenpool herstellt, der diese Konfiguarationsdaten enthält. Dies kann bei einer Telefonanlage zweckmäßigerweise eine Datenverbindung über die Telefonleitung selbst sein, in anderen Fällen je nach zu konfigurierendem Gerät kann eine e-mail oder TCP/IP Verbindung zweckmäßig sein. Der Datenpool ist in den meisten Fällen die Festplatte eines Rechners, der als Server funktioniert.

Weiter ist das erfinderische Konzept dazu geignet, Geräte zeitweise, beispielsweise für die Abwesenheit während des

Urlaubs stillzulegen und somit vor Mißbrauch zu schützen. So kann die SMART Card einen Befehl an das Gerät absetzen, dieses stillzulegen, also keine weiteren Befehle bis auf einen 'wake-up' Befehl anzunehmen und zu verarbeiten. Dies nutzt in besonderer Weise die Fähigkeit aus, die SMART Cards bieten, in sehr variabler Form Objekte zu definieren und ihnen bestimmte Methoden als auszuführende Befehle zuzueignen.

Durch Anwendung des Verfahrens nach der vorliegenden Erfindung können Produktionsprozesse für Geräte erheblich vereinfacht werden, Kosten für die Lagerhaltung gesenkt und die Logistik bei der Verteilung der Geräte in den Handel bzw. an den Endkunden vereinfacht werden, da die Geräte einheitlich hergestellt, gelagert und verteilt werden können. Desweiteren werden die Anforderungen an den äußeren Diebstahlschutz gesenkt, da die Geräte ohne zugehörige SmartCard weitgehend nutzlos sind, was einen erheblichen Fortschritt gegenüber dem derzeitigen Schutz gegen Mißbrauch durch Eingabe eines Paßworts darstellt.

Weitere Aktionen, die bei einem unbefugten Zugriff auf das Gerät autonom ohne Kenntnis des Benutzers und angestoßen durch ein entsprechendes Applet auf der SmartCard veranlasst werden können, sind beispielsweise die Absetzung einer e-mail an eine vorbestimmte Adresse oder das Absetzen eines bestimmten Warnsignals (ping) an eine zuständige Stelle im Unternehmen, sofern das Gerät entsprechend vernetzt ist.

Weiter kann der Gegenstand der vorliegenden Erfindung in Hardware, Software oder einer Kombination aus beiden realisiert werden. Eine beliebige Art von Computersystem oder Computergeräten ist dafür geeignet, das erfindungsgemäße Verfahren ganz oder in Teilen durchzuführen. Eine realisierbare Hardware-Software Kombination wäre ein normaler Computer mit einem

Computerprogramm, das, wenn es geladen und ausgeführt wird, den Computer derart steuert, daß er das erfindungsgemäße Verfahren ganz oder in Teilen ausführt.

Die vorliegende Erfindung kann auch in ein Computerprogrammerzeugnis eingebettet sein, das sämtliche Merkmale enthält, die eine Implementierung der hierin beschriebenen Verfahren ermöglichen, und die, wenn sie in ein Computersystem geladen wird, dazu imstande ist, diese Verfahren auszuführen.

Computerprogrammeinrichtungen und Computerprogramme bedeuten im vorliegenden Kontext beliebige Ausdrücke in einer beliebigen Sprache oder Notation oder einem beliebigen Code eines Satzes von Anweisungen, die ein System mit einer Informationsverarbeitungsmöglichkeit dazu veranlassen sollen, von den folgenden Funktionen

a) Umsetzung in eine andere Sprache oder Notation oder einen anderen Code,

b) Reproduktion in eine unterschiedliche materielle Formeine bestimmte entweder direkt oder nacheinander oder beide durchzuführen.

Es ist offensichtlich, daß die Aktionen, die durch die SMART Card ausgelöst werden können, von Gerät zu Gerät sehr unterschiedlich sein können, und dem jeweiligen Zweck der Verriegelung im Sinne einer temporären Stilllegung bzw. der Konfiguration der Geräte angepaßt sein müssen.

P A T E N T A N S P R Ü C H E

1. Verfahren zum Festlegen grundlegender Verfügungsmöglichkeiten über den Betrieb von Geräten, deren Betrieb mit einer elektronischen Gerätesteuerung steuerbar ist,gekennzeichnet dadurch, daß es die Schritte enthält:

   Aufbauen (110) einer Verbindung (19) zwischen einer, mit Verschlüsselungsdaten versehenen, personenbeziehbaren Authentifizierungseinrichtung (16) und einer Logikeinrichtung (20), die die elektronische Gerätesteuerung steuern kann,

   Prüfen (120, 140) der Daten in der Authentifizierungseinrichtung (16) vor dem Betreiben des Geräts,

   Zuordnen von vorbestimmten, der Authentifizierungseinrichtung (16) zugehörigen Verfügungsmöglichkeiten über das Gerät,

   Zulassen (150) der für die Authentifizierungseinrichtung (16) vorbestimmten Verfügungsmöglichkeiten abhängig vom Ausgang der Prüfung.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Verfügungsmöglichkeiten wenigstens eine der folgenden Möglichkeiten umfassen:den Betrieb des Geräts (12) zu unterbinden,den Betrieb des Geräts (12) freizugeben, oder eine Konfiguration des Geräts (12) zu ermöglichen.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Verbindung (19) unter Vermeidung zwischenliegender Softwareschichten gebildet ist.

4. Verfahren nach dem vorstehenden Anspruch, enthaltend den Schritt, wenigstens eines der folgenden Merkmale von der Authentifizierungseinrichtung (16) zu lesen: Firmware-Programme, gerätespezifische Befehlssequenzen für die Ausführung bestimmter, gerätespezifischer Funktionen,kryptographische Schlüssel,kryptographische Algorithmen,individuelle Entscheidungslogik.

5. Verfahren nach einem der vorstehenden Ansprüche 1 bis 4 zum Konfigurieren von Geräten (12) durch berechtigte Personen, wobei nach einer erfolgreichen Authentifizierung gerätespezifische Konfigurationsdaten von der Authentifizierungseinrichtung (16) nach einem der beiden vorstehenden Ansprüche oder über ein Netzwerk in das Gerät (12) geladen werden.

6. Gerät (12) zur Durchführung des Verfahrens nach einem der vorstehenden Ansprüche.

7. Authentisierungseinrichtung (16), eingerichtet für eine Authentifizierung einer Person oder einer Personengruppe in dem Verfahren nach einem der Ansprüche 1 bis 4.

8. Authentisierungseinrichtung (16) nach dem vorstehenden Anspruch, dadurch gekennzeichnet, daß sie in Form einer SmartCard realisiert ist.

9. System zum Festlegen grundlegender Verfügungsmöglichkeiten über den Betrieb von Geräten (12), deren Betrieb mit einer elektronischen Gerätesteuerung steuerbar ist, enthaltend wenigstens ein

Gerät (12) nach Anspruch 6, und eine Authentisierungseinrichtung (16) nach Anspruch 7 oder 8.

10. Computerprogramm, enthaltend Programmcodebereiche zur Durchführung oder Vorbereitung der Durchführung der Schritte des Verfahrens gemäß einem der Ansprüche 1 bis 4, wenn das Programm in einen Computer geladen wird.

Z U S A M M E N F A S S U N G

Verfahren und Vorrichtung zum Festlegen grundlegender Verfügungsmöglichkeiten über den Betrieb von elektronisch angesteuerten Geräten (12) mithilfe einer gegebenenfalls übertragbaren, personenbeziehbaren Authentisierungseinrichtung (16), basierend im wesentlichen auf drei Komponenten, die während des erfinderischen Verfahrens ausgenutzt werden, nämlich einer Erweiterung der Gerätehardware um Funktionen, die die Verfügungsmöglichkeiten, nämlich insbesondere die individuelle Konfiguration und die Stilllegung der Geräte erlauben, einer hardwarenahen Schnittstelle zu einem Lesegerät (18) für die Authentifizierungseinrichtung (16), wie etwa einem Smartcard-Reader, der den Zugriff auf diese Funktionen durch eine Smartcard (16) erlaubt, und der Authentifizierungseinrichtung (16) selbst, die in der Lage ist, über die definierte Schnittstelle auf die Konfigurations-/ und / oder Stilllegungs- bzw. Inbetriebnahmefunktionen der Hardware des Gerätes unmittelbar zuzugreifen.
Die Legitimation zur Konfiguration /Stilllegung und (Wieder)-Inbetriebnahme des Geräts erfolgt über den Abgleich von Schlüsseln, die auf der SmartCard (16) bzw. in der in einem ROM (14) des Geräts (12) gespeichert sind.
(Fig. 1)

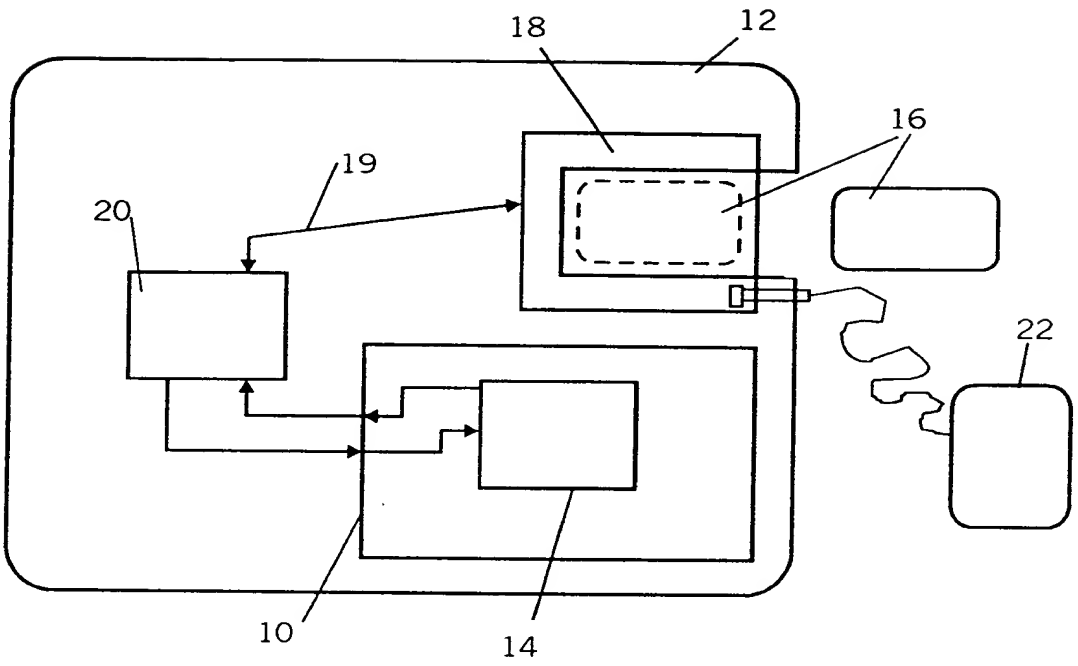

FIG. 1

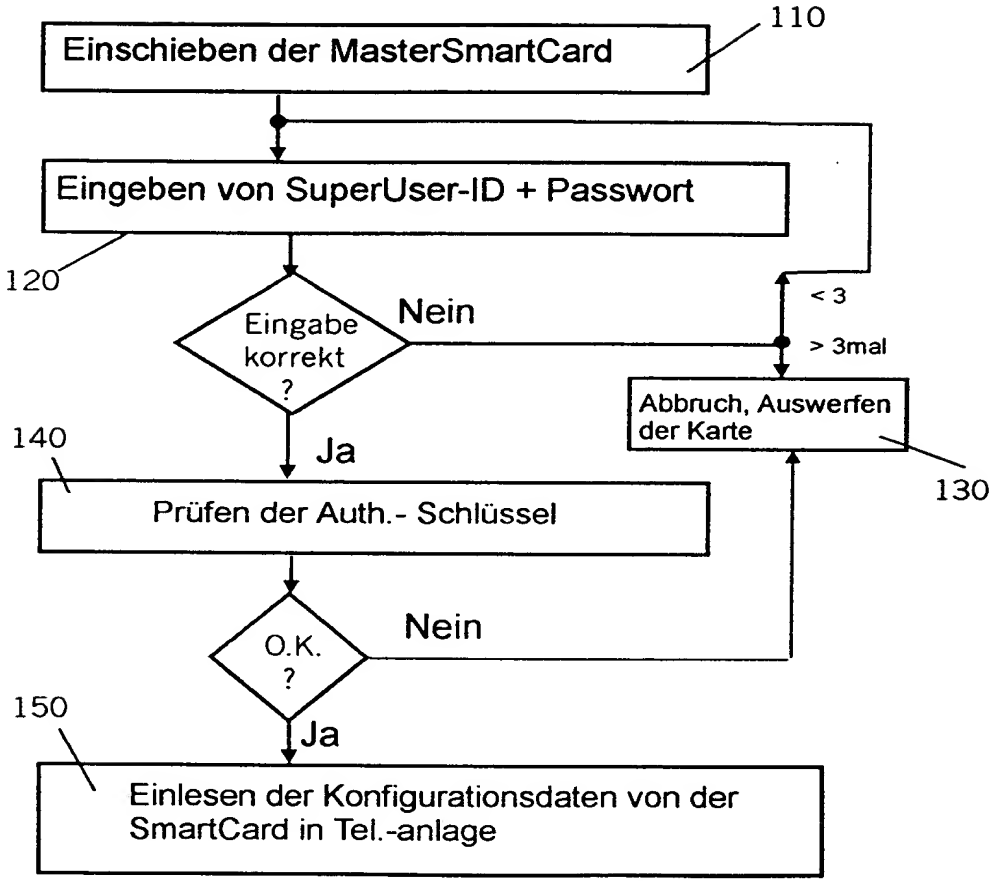
Einschieben der MasterSmartCard
110
Eingeben von SuperUser-ID + Passwort
120
Eingabe korrekt ?
Nein
< 3
> 3mal
Abbruch, Auswerfen der Karte
130
Ja
140
Prüfen der Auth.- Schlüssel
O.K. ?
Nein
Ja
150
Einlesen der Konfigurationsdaten von der SmartCard in Tel.-anlage

FIG. 2